Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

THE
AMERICAN
MATHEMATICAL MONTHLY.

Entered at the Post-office at Springfield, Missouri, as Second-class Mail Matter.

VOL. III. AUGUST-SEPTEMBER, 1896. No. 8-9.

APPLICATIONS OF SUBSTITUTION GROUPS.

By G. A. MILLER, Ph. D., Paris, France.

Lagrange seems to have been the first to give a clear statement and at least a partial proof[*] of the following fundamental

THEOREM I. *The number* (N) *of different formal values which are obtained by permuting the n elements of a given function in every possible manner is a divisor of* $n!$.[†]

About thirty years later Ruffini proved that N cannot have the values 3 or 4 when $n=5$, in his work, "*Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto,*" Bologna, 1799. He thus proved also that N cannot be equal to every divisor of $n!$.

As it was known that the value of N is the quotient obtained by dividing $n!$ by the order of the largest substitution group which transforms the function into itself it became an important problem to determine all the possible orders of the substitution groups of n elements, especially since it was believed that this would throw light on the solution of the general equation of the n^{th} degree. This problem has been solved only for small values of n.

The given theorem of Lagrange indicates the most direct application of substitution groups and therefore naturally furnished the starting point for the early investigations in this subject. It may be readily proved in the following manner.[‡]

Let ψ, the given function, be unchanged only by the substitutions in the first row of the following rectangle. (These form a group, for the product of any two leaves ψ unchanged and is therefore found in this row.)

---

[*] The proof given by Lagrange in his article, "*Reflexions sur la resolution algebrique des equations,*" Memoires de l'Academie de Berlin, 1770 and 1771, seems to have been generally considered as complete. Cf. Mathieu, Comptes Rendus, 46, page 1047. Burkhardt, on the contrary, seems to regard it as incomplete. Cf. Zeitschrift fur Mathematik, 1892, page 141.

[†] $n!=1.2.3......n$.

[‡] Cf. Netto's Theory of Substitutions (Cole's edition) §41.

$$\begin{array}{llll}
s_1=1 & s_2 & s_3 \ldots\ldots\ \ldots\ldots s_a & \\
t_2 & s_2 t_2 & s_3 t_2 \ldots\ldots\ldots\ldots s_a\, t_2 & \\
t_3 & s_2 t_3 & s_3 t_3 \ldots\ldots\ldots\ldots s_a\, t_3 & \\
\vdots & \vdots & \vdots\ \ldots\ldots\ldots\ldots\ \vdots & \\
\vdots & \vdots & \vdots\ \ldots\ldots\ldots\ldots\ \vdots & \\
\vdots & \vdots & \vdots\ \ldots\ldots\ldots\ldots\ \vdots & \\
t_m & s_2 t_m & s_3 t_m \ldots\ldots\ldots\ldots s_a\, t_m & m=\dfrac{n!}{\alpha}.
\end{array}$$

ψ will assume the same formal value if any one of the substitutions of a given row is applied to it, for the first factor leaves it unchanged and the second factor is the same throughout the row. If we assume that t_β ($\beta=2, 3, \ldots\ldots m$) is not found in a preceding row the substitutions of the rectangle are all different, for from

$$t_{\beta_2}s_{\gamma_2}=t_{\beta_1}s_{\gamma_1} \qquad (\beta_2 \geqq \beta_1 \leqq m)$$

we would have $\qquad (\gamma_1, \gamma_2, \gamma_3 \leqq \alpha)$

$$t_{\beta_2}=t_{\beta_1}s_{\gamma_3}.$$

This is impossible unless $\beta_1=\beta_2$ and $s_{\gamma_3}=1$. In this case $t_{\beta_2}s_{\gamma_2}$ and $t_{\beta_1}s_{\gamma_1}$ occupy the same place in the given rectangle.

Since there are just $n!$ substitutions of n elements the given rectangle contains each substitution once and only once. If t_{β_1} and t_{β_2} would transform ψ into the same function (ψ_1) then would the products of all the substitutions in the rows containing t_{β_1} and t_{β_2} into a substitution* t_γ which transforms ψ_1 into ψ give 2α different substitutions that transform ψ into itself. This is contrary to the hypothesis. Therefore $N=m=$ a divisor of $n!$.

One of the best known functions to which these elementary principles of substitution groups are commonly applied is the anharmonic ratio of four points.† If the four points are represented by A, B, C, and D, their anharmonic or cross ratio may be represented by

$$\psi\equiv\frac{AB}{CB}\div\frac{AD}{CD} \text{ or } \frac{AB.CD}{AD.CB}.$$

It is required to find the number of formal values of ψ when the points are interchanged in every possible manner. We may do this by dividing $4!=24$ by the order of the largest group of degree four that transforms ψ into itself. Since ψ is unchanged by the substitution $AB.CD$ and also by the substitution

---

*Since the rectangle contains all the possible substitutions of n elements, it must contain the inverse of each of its substitutions. We shall always consider n to be a finite number.

†Cf. Harkness and Morley's.

$AD.BC$, it must be unchanged by the group generated by these substitutions, viz., by $(AB.CD)_4$. We know that there are only three groups* of degree four which include $(AB.CD)_4$ and that these contain either a substitution of the form AB or one of the form ABC. As no such substitution transforms ψ into itself $(AB.CD)_4$ is the largest group that has this property. The number of different values of ψ is therefore $24\div4=6$.

To find these six values of ψ we may arrange the substitutions of four elements as follows :

1	$AB.CD$	$AC.BD$	$AD.BC$
AB	CD	$ACBD$	$ADBC$
AC	$ABCD$	BD	$ADCB$
AD	$ABDC$	$ACDB$	BC
ABC	ACD	BDC	ADB
ACB	BCD	ABD	ADC

Since all the substitutions of a row transform ψ into the same function we can find the six formal values of ψ by applying to it the six substitutions of the first column in this rectangle.† We thus obtain the following, in order :

$$\frac{AB.CD}{AD.CB}=k;\ \frac{BA.CD}{BD.CA}=\frac{\dfrac{BA.CD}{AD.CB}}{\dfrac{AD.CB-AB.CD}{AD.CB}}=\frac{k}{k-1};\ \frac{CB.AD}{CD.AB}=\frac{1}{k}.$$

$$\frac{DB.CA}{DA.CB}=\frac{AD.CB-AB.CD}{AD.CB}=1-k;\ \frac{BC.AD}{BD.AC}=\frac{1}{1-k};\ \frac{CA.BD}{CD.BA}=\frac{k-1}{k}=1-\frac{1}{k}.$$

This example furnishes also a clear illustration of what we mean by "*different formal values.*" The six given values of ψ are all different as to form but k may have such values that they are not all really different. E. g., if $k=-1$, they coincide in pairs. In this case the ratio is called *harmonic*. If k=an imaginary cube root of -1, they coincide in triplets and the ratio is called *equianharmonic*.

It should be observed that each one of the four subgroups of $(ABCD)$all, which are of the form (ABC)all, has one substitution in each row. Hence the following

Theorem II. *The six different formal values of an anharmonic ratio of four points may be obtained by transforming any three of its points symmetrically.*

---

*It is evident that the function is not symmetric. It would therefore only be necessary to examine it with respect to the other two groups.

†This is clearly only one of the 4096 different ways in which the six transforming substitutions may be selected.

If G is the largest group which transforms a function (ψ) into itself we say that *ψ belongs to G*. The same relation is also expressed by saying that *G belongs to ψ*.[*] The former of these two expressions is to be preferred since only *one group belongs to any given ψ while an infinite number of functions belong to any given G*. This may be readily proved as follows :[†]

We first suppose that G is the symmetric group of n elements. Every symmetric function of these elements will then belong to G. That their number is infinite, follows directly from the fact that both a and b can have an infinite number of different values without impairing the symmetry of the following functions :[‡]

$$x_1^a+x_2^a+x_4^a+\dots\dots+x_n^a+bx_1x_2x_3\dots\dots x_n \quad\dots\dots\dots\dots\quad A.$$

We may now suppose that G consists of a single substitution, viz., identity. In this case every function of the n elements which is changed in form by each substitution of these elements belongs to G. If we suppose that a_1, a_2, a_3, ..., a_n represent n different given numbers, the following function belongs to G:

$$a_1x_1+a_2x_2+a_3x_3+\dots\dots+a_nx_n \quad\dots\dots\dots\dots\dots\dots\quad B.$$

We may now assign all the possible values of a_1 with the exception of the finite number of values represented by a_2, a_3, ..., a_n. In this way we obtain an infinite number of functions belonging to G.

We finally suppose that G represents any other group whose order is g. If we apply the substitutions of G to any one of the functions of B we obtain g different functions, ψ_1, ψ_2, ψ_3, ..., ψ_g. In any of the functions A we may suppose $n=g$ and the x's, in order, replaced by these ψ's. The resulting function belongs to this G. It is clear that we obtain an infinite number of such functions even by using a particular function of either A or B. We did not prove that all the functions belonging to G can be obtained in this way. In fact, this is not the case. As it follows from the definition that only one group belongs to a given function the proof is complete.

We have thus far only considered the relations between groups and functions when all the elements of the function which are permuted and no others are explicitly contained in the corresponding group. We have also only considered the number of values of a function when its elements are permuted according to the symmetric group. That the arguments which were employed apply to much more general cases may be illustrated by means of the following well-known Trigonometry formula

$$\text{Sin}\,\frac{A}{2}=\sqrt{\frac{(s-b)(s-c)}{bc}}.$$

---

[*] Cf. Netto, Theory of Substitutions (Cole's Edition) §28.

[†] Ibid, §30.

[‡] If a and b are complex numbers, A represents ∞^4 different functions.

If we regard the first member of this equation as a function of the three angles A, B, C of a triangle it belongs to the group (BC) and is therefore a three-valued function of the angles. The second member belongs to the group (bc) and is therefore a three-valued function of the sides. Hence the formula says that *a given three-valued function of the angles is equal to a given three-valued function of the sides.*

As no special properties were imposed upon any the sides or angles in deriving the formula the three different values of the angles must correspond separately to the three different values of the sides. It remains only to find the substitutions which transform the given formula into the other two. To do this we may arrange the substitutions of the angles and the sides, in the usual manner, as follows :

$$\begin{array}{ll} 1 & BC \\ AB & ABC \\ AC & ACB \end{array} \qquad\qquad \begin{array}{ll} 1 & bc \\ ab & abc \\ ac & acb \end{array}$$

Since the substitutions of a row transform the corresponding functions in the same way and the rows of the two rectangles evidently correspond in order, we may effect the required transformation by any two substitutions such that one belongs to the first and the other to the second of the following two rows :

$$AB.ab,\ AB.abc,\ ABC.ab,\ ABC.abc$$
$$AC.ac,\ AC.acb,\ ACB.ac,\ ACB.acb$$

If we use the last one of each of these rows we have the rule frequently given in the text-books, viz., "The corresponding formulas for the other two angles may be obtained from this by the cyclical interchange of the letters."

The given formula might also be studied by employing a single group in place of two. The most convenient group is the intransitive group of degree six and order 36 which is obtained by multiplying the symmetric group of the angles into the symmetric group of the sides.* Since the given formula is transformed into itself only by the following four substitutions of this group

$$1,\ BC,\ bc,\ BC.bc,$$

it is a nine-valued function with respect to this group.† Since substitutions of this group transform the first member of the given formula into its three values without affecting the second member, these nine values may be arranged into three triplets, each of which has the same second member. By very simple trials we can show that six of these relations are absurd. Since three must be true the remaining relations are the required formulas.

---

*Cf. This journal, Vol. II, page 307.

†This may be proved in exactly the same way as Lagrange's theorem was proved.

Since similar remarks apply to a large number of the other Trigonometry formulas, it is clear that these formulas can be discussed in a more general and more definite manner by presupposing a thorough knowledge of the given elementary principles of substitution groups.

It is also easy to show that many problems of factoring can be discussed more completely by presupposing a knowledge of these groups. The following is a very simple illustration :

$$a^2-b^2-c^2+2bc=(a+b-c)(a-b+c) \ldots\ldots\ldots\ldots \ldots. C.$$

The expression belongs to the group (bc) and is therefore a three-valued function; its factors belong to the groups (ab) and (ac) respectively and are therefore also three-valued functions. Hence C indicates an equality between a given three-valued function and the product of two other three-valued functions. These functions belong to three distinct groups. Arranging the substitutions of these groups in the usual manner, we have

$$\begin{array}{ll} 1 & bc \\ ab & abc \\ ac & acb \end{array} \qquad\qquad \begin{array}{ll} 1 & ab \\ ac & abc \\ bc & acb \end{array} \qquad\qquad \begin{array}{ll} 1 & ac \\ ab & acb \\ bc & abc \end{array}$$

The three values of the given expression* may be obtained by applying to it one substitution from each of the three rows of the first rectangle, e. g., the first column. The factors of these transforms may evidently be found by applying the same substitutions to the given factors. Since ab and ac transform one of the factors into itself it follows that the three conjugate expressions contain only three distinct linear factors, viz., the three values of any one of them.

These observations indicate how we may readily determine the total number of substitutions by means of which the factors of all the conjugates of a given expression may be found from those of the given expression. They have brought us in contact with, at least, three important questions, viz. :

1. What relations exist between the factors of a system of conjugate expression ?
2. What relations exist between the groups of the factors and the group of the expression ?
3. To what extent may these relations be utilized in the process of factoring ?

---

*The same idea is expressed by "the three conjugates of the given expression" or by "the three transforms of the given expression."